実践・全社情報セキュリティ強化

TDK 株式会社

■ 執筆者Ｐｒｏｆｉｌｅ ■

中村　眞一

1983 年 4 月	TDK 株式会社　入社
	情報システム部システム開発担当
1986 年 11 月	TDK 米国（NY,CA）へ出向
1995 年 4 月	情報システム部システム開発リーダー
2008 年 7 月	TDK 中国（上海）へ出向
2011 年 4 月	情報システム部 IT インフラリーダー
2015 年４月	情報セキュリティ委員会事務局長兼務

■ 論文要旨 ■

2015 年 1 月筆者が急遽 TDK 全社の情報セキュリティ事務局長の命を受けた後、2015 年４月から 2016 年３月までグローバルで情報セキュリティ強化に取組んできた奮闘内容をまとめました。決して先進的な事例ではありませんが、IT 施策以上に、従業員へのセキュリティ意識向上に重点的に取組んだ結果、ＰＣやスマートフォン紛失、ウイルス感染などの情報セキュリティ事故を対前年比で半減する事ができました。
具体的には、全社体制の確立、セキュリティ月報の発刊、セキュリティ読み合せ、USB 記録デバイス制限、サイバー攻撃メール訓練などコストをほとんどかけない施策も多く、富士通ファミリ会会員企業の皆様の参考になれば幸いです。
又、世界的なサイバーセキュリティの脅威を鑑み、僭越ではございますが、日本政府への提言も書かせていただきました。

■ 論文目次 ■

１．はじめに ……《 3》

２．目標設定 ……《 3》

３．体制作りと見える化……《 4》

３．１　体制見直し

３．２　情報セキュリティ月報

３．３　情報セキュリティ管理者会議

４．重点施策展開……《 6》

４．１　情報セキュリティ遵守事項読み合せ

４．２　USB記録デバイス制限

４．３　その他施策

４．４　事故件数削減結果

５．施策外部評価 ……《 10》

６．日本政府への提言……《 11》

７．終わりに ……《 11》

参考資料……《 13》

■ 図表一覧 ■

（図１）2015/4～2016/3の情報セキュリティ委員会事務局の目標……　《　3》

（図２）全社の情報セキュリティ管理体制……　《　4》

（図３）米国社長会議での説明風景……　《　5》

（図４）グローバル管理者会議風景……　《　6》

（図５）海外現地法人従業員セキュリティ教育風景……　《　6》

（図６）海外拠点のレーダーチャート例……　《　9》

（図７）グローバル主要メンバーと……　《 12》

（図８）情報セキュリティ月報例……　《 13》

（図９）情報セキュリティ遵守確認シート……　《 14》

１．はじめに

「中村君、全社情報セキュリティ委員会の事務局リーダーをやってくれないか？」と、2015 年 1 月上司からの突然の問いかけに、驚きながらも即座に「わかりました。」と応えてしまっていた。この時点では、情報セキュリティに関しての知識も考えも無かったが、入社以来いろいろな新しいテーマにチャレンジさせてもらっていた事と、何とかなるさという楽天的な性格がそう反応させたのかもしれない。ただ、全社的に情報セキュリティ事故が増加している事は周りから聞いていたし、現状のままではまずいという危機意識があった事は、上司に見抜かれていたのかもしれない。

初めての職責に奮闘しながら 1 年半後、今度は「富士通論文に応募してみないか？」である。我が社の事例は地味なものばかりだが、取組の効果は数字となって表れている。他社でも参考になる内容かもしれない。又、「わかりました」と答えてしまった。

個人的にも、この固いテーマを少しでもわかりやすく、シンプルに楽しく取組んできたつもりである。論文という形に慣れない面はお許しいただきたい。

まず弊社のセキュリティの規模を理解いただくために全社の PC 台数(概算)を記載しておく。

国内：10,000 台、海外：40,000 台　（連結対象子会社約 130 社合計）

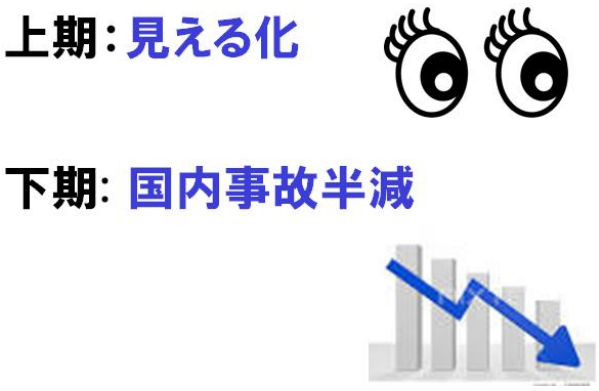
40 行

２．目標設定

2015 年 2 月、まず情報セキュリティ委員会事務局リーダーとして、事務局メンバーを一つにまとめるための目標設定に取組んだがしばらく悩んだ。当然、委員会事務局メンバーにも相談したが納得できる明確な目標設定には至らない。過去の目標も確認したが情報セキュリティ強化や機密情報資産管理徹底など漠然とした表現が多くこれではメンバー間で目標値（ゴール）認識が同じにならないと感じた。しばらく悩んだ末、情報セキュリティの究極の目標は情報セキュリティ事件、事故をゼロにする事だとの結論に至った。品質管理と同じ考え方で良いのではないかと自分なりに結論づけたのである。

当時は PC やスマートフォン、USB 紛失、メール誤送信、ウイルス感染などが月に数件発生し、かつ増加の傾向にあった。そこで「下半期（2015/10-2016/3）の事故件数を対前年比で半減させるのが我々の目標」と宣言した。勿論その時点では具体的方策も自信も何も無い状態。突然の高い目標設定にみんな驚いていたが、結果的にはこの目標設定が成功の鍵だったと感じている。この下半期目標達成のため、上半期（2015/4-2015/9）を体制整備や見える化、情報共有を進める準備期間と位置付けた。（図１）

（図１）2015/4～2016/3 の情報セキュリティ委員会事務局の目標



実は、IT 部門担当者に情報セキュリティの相談をすると、ウイルスメール検知や USB 使用制限などセキュリティ施策の話が先行する事が多い。でもこれらは目標ではなく手段である。私は、IT 部門も兼務しており日頃からメンバーには手段よりも目的や目標、つまり何のためにやっているかを常に意識しよう！と言っている。これをおろそかにすると、いつのまにかシステムを導入する事事体が目的になってしまうケースが多々ある。

実は、情報セキュリティ委員会事務局メンバー6 名の内、4 名が IT 部門出身者で構成されており、話し合いの中で同じ傾向を感じ、あえてこの目標設定を大事にした。ゴールが明確になった事で、メンバーの意識統一だけでなく後述する施策の優先順位づけが容易になった。ただ、この目標は各部門が正直に事故報告をしてこなくなる事を懸念し全社には公開はしなかった。

３．体制づくりと見える化

３．１ 体制見直し

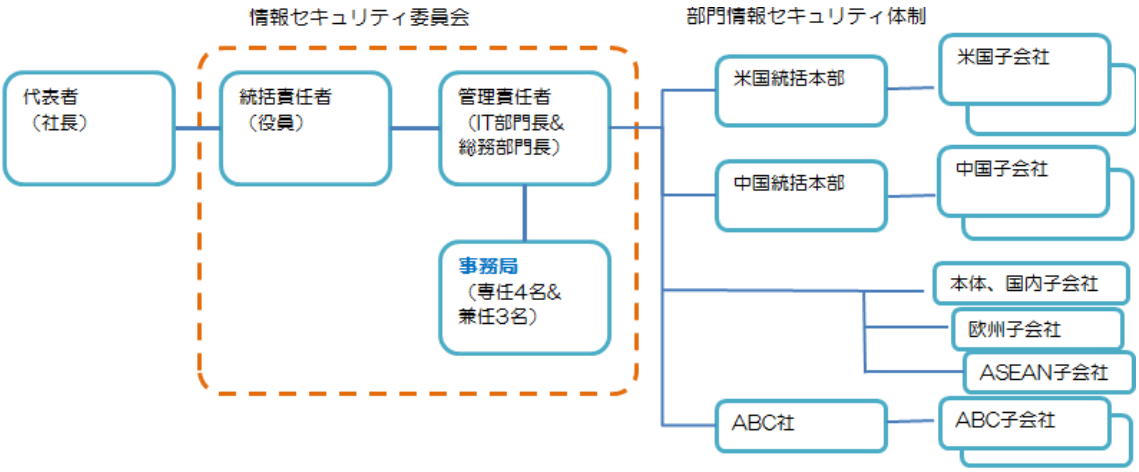
まず、最初に着手したのは、全社の情報セキュリティの体制の見直しである。部門毎、子会社毎に情報セキュリティ責任者、管理者、担当者を明確にし、部門、子会社内の情報セキュリティの統制、施策実行の役割を担ってもらう。勿論現業との兼任でも良い。但し、選任にあたり下記ルールは徹底してもらった。

① 情報セキュリティ責任者は部門責任者又は子会社社長
② 情報セキュリティ管理者は課長職以上で IT 部門以外から選出。
③ 情報セキュリティ担当者は複数名可。IT 部門要員でも OK。

周知の理由は、情報セキュリティは全社を挙げて取組むテーマである事を明確にしたかった事と情報セキュリティ管理者は様々な施策を現場に定着させる重要な役割を担うため、組織内メンバーを統制できる方を選定してもらいたかったからである。

私は情報セキュリティはトップダウンの推進しかありえないテーマだと思っている。ボトムアップで部門それぞれが個別の施策をとるものではない。全社で統一した考え方、施策を展開する事が何より重要と考え、この体制の見直しを全子会社にお願いした。
結果、グローバルで総勢 280 名に及ぶバーチャルな情報セキュリティ組織が出来上がった。

（図 2）全社の情報セキュリティ管理体制



３．２ 情報セキュリティ月報

体制が明確になった後、着手したのが見える化の第一歩、「情報セキュリティ月報」の発刊である。この月報は全社の情報セキュリティメンバーに TDK の情報セキュリティの現状を理解してもらうための「見える化」の道具と位置付けた。内容は全社で起こった情報セキュリティ事故の内容、部門別ウイルス検知状況、そして後述する情報セキュリティ各種施策の部門別進捗状況、その他事務局からの連絡事項などからなる。情報セキュリティメンバーへの情報伝達だけでなく、自分の部門が全社レベルに比べて遅れているのかどうかも理解していただくものとなっている。又、セキュリティ事故の内容もある程度公開する事で自部門のセキュリティ活動に活かしていただく事も狙っている。

月報として月 1 回の発刊は情報セキュリティ事務局担当者の負担にはなっている様だが、毎月担当者を変えるなどして現在も継続している。これにより本社も現場もある程度同じ問題意識を持てるようになったのは間違いない。

半年間は日本国内向けの月報であったが、その後海外現地法人向けの英語版も発刊している。（情報セキュリティ事務局メンバーの英語力向上にも役立っている。）

巻末に月報のサンプル（図８）を掲載させていただいた。

３．３ 情報セキュリティ管理者会議

月報の発行と並行して、部門情報セキュリティ管理者会議の定期開催も実施した。これは全社の情報セキュリティ責任者（役員）と部門セキュリティ管理者が一同に会し、意見を交換する場にしている。後に記載する様々なセキュリティ施策もこの会議で事前の了解をいただいた上で進めており、重要な意思決定の場となっている。

海外においては、情報セキュティ事務局から地域毎の経営会議や主要現地法人に直接出向き、セキュリティ責任者（現地法人社長）やセキュリティ管理者の方々の理解を得る活動を継続している。（図３、図４参照）　中には、現地法人社長から現地従業員向けのセキュリティ教育を直接行って欲しいなど要望もいただき、実施する事もある。（図５参照）

難しい施策のお願いや交渉事は Face to face でコミュニケーションする事が結果的には近道であるといつも感じる。いくら IT が発達してもこれは変わらない。

（図３）米国社長会議での説明風景

（図４）グローバル管理者会議風景

（図５）海外現地法人従業員セキュリティ教育風景

４．重点施策展開

４．１ 情報セキュリティ遵守事項読み合せ

実は、情報セキュリティ事故半減を目標に定めた時から、目標達成のためには従業員のセキュリティへの心掛け、意識の向上が一番大事なポイントと感じていた。情報セキュリティの IT 施策に 100%の仕組みはなく、最後の砦は従業員の意識である。当時、事故として多かった PC や携帯電話、スマートフォンの紛失はまさにその典型で、どんな IT ツールを使っても紛失自体を防ぎようがない。

又、紛失を防止するルールを作ったとしても全社員に周知する事やルール遵守を継続してもらうのは決してたやすい事ではない。現状行っている年次のセキュリティ教育(e-Learning)だけでは十分理解できていないという現場の声も聞こえていた。

そこで考えたのが「読み合せ」である。これは、従業員に普段から意識して欲しい遵守

事項をわかりやすい短文（1 ページ）にまとめ、月に 1 度、係や課など小規模会議等の冒頭などで誰かが口に出して読み、皆さんがそれを耳にし再認識する活動である。簡単に読める様、遵守事項は 10 項目程度、2-3 分で読める内容にし、全社に配布した。例えば、

・携帯電話、スマートフォンはネックストラップなどで落下防止します。
・PC 持参で飲み会に参加しません。参加せざるを得ない時は上司の了解を得、
　二次会には参加しません。
・飲んだ後の SNS 投稿はしません。
・ウイルス感染したかもと感じたら、ネットワークを遮断してから IT 部門に連絡します。

など、身近な事柄について遵守を宣言をする文面にした。
又、読み合せの徹底を図るため、各部門から参加者を毎月事務局に報告をもらうようにし、部門別の読み合せの実施率も先述のセキュリティ月報で共有している。
2015 年 6 月から開始したこの取組みだが、当初は抵抗のある部門や人もいたが、今では国内従業員の９０％が毎月取組んでくれている。
巻末に遵守読み合せシートの一部（図９）を掲載させていただいた。

ただ、定着が進んできたかと感じ始めていた 2015 年 9 月頃から「読み合せに飽きてきた。」という声が従業員の皆さんから届くようになった。確かに同じ文面を毎月読み聞かされるのは飽きてしまう。そこで思いついたのが「標語版」である。つまり、交通標語と同じで遵守事項を５－７－５形式で表現したもの。標語の中には関西弁なども織り交ぜ、少しは楽しく読める工夫もした。例えば、「パスワード書いて貼ったらあきまへん。」ふざけるな！との反発も覚悟をしていたが、以外にも反発はなく、「これ作ったの中村さんでしょ」と。むしろ好意的な？反響が寄せられたりした。

その後も、再度の「飽きた」の声に応えるべく、「クイズ版」（大事な部分は空白にしたもの）も作成提供している。どの読み合せ版を使うかは各部門の判断に任せており、今期になってからは、セキュリティ事故も大幅に削減された事から、読み合せとり止めの要望も部門情報セキュリティ管理者からはあがっていたが、止める代わりに新たに、分割版と称して 10 項目を 3 ヶ月かけて読む「短縮版」を提供し読み合せは継続している。

ただ、この「読み合せ」は国内では想定以上の効果を生んでくれたが、海外への展開は苦労しているのが実態。勿論英訳版や中国語版は作成はしたが、「読み合せ」という文化がない国の方々にこれを強いるのは難しい。ただ、年次教育だけでは不十分という点では海外現地法人社長の皆さんも理解してくれており、地域毎に少しやり方を工夫しながら実施、報告してくれている。但し海外における実施率はまだまだ発展途上と言うべきだろう。

４．２ USB 記録デバイス制限

もう一つの重点施策として、USB 記録デバイスの利用制限に取組んできた。ご存知のように USB 記録デバイスは大変便利な道具ではあるが、情報セキュリティの面では、情報漏洩や紛失など大きなリスクを持つツールである。過去、社内で USB 記録デバイスに関する事件も数件発生しており、緊急を要する課題でもあった。

社内ではルール上原則利用禁止とはしていたものの、利便性の面からシステムによる使用制限にまでは至っていなかった。事前に情報セキュリティ管理者会議でシステムによる制限を説明し合意に至っていたが、実際に始めてみると、USB 記録デバイスが利用できる PC の削減が思うように進まなかった。特に初回の調査（棚卸し）では、何かの際に使えな

いと不便。や取引先との大容量データ交換や、既存生産設備とのデータ交換等様々な理由が挙げられ、2015 年 9 月末時点で USB 記録デバイスが利用できる PC は全体の 40%にまでしか削減できなかった。情報セキュリティ事務局内部では、2016 年 3 月末で 20%の目標を掲げていたのだが、これとは大きく乖離する結果であった。

ただ、内訳を見ると、大幅に削減できている部門とそうでない部門とでかなりのバラつきがある事がわかり、2015 年 10 月に開催した、情報セキュリティ管理者会議で削減が進まない部門、子会社の情報セキュリティ管理者には状況報告と 3 月末までの削減計画をセキュリティ責任者（役員）の前で発表していただいた。その後社長にも全面的にバックアップいただいた事も功を奏し、2016 年 3 月末で 20%の目標を何とか達成する事ができた。
現在は更に削減が進み、2016 年 8 月末時点では、全体の９%にまで削減が進んでいる。
IT 面でも USB 利用専用の共有 PC を各拠点に配置したり、後述の社外とのデータ交換用のクラウドサービスや個人用ファイルサーバーを提供したり、社内クラウド型の共有ファイルサーバーを提供したりと様々な IT 環境もタイムリーに提供できた事も成功の要因と考えている。

現在は、USB 記録デバイス個体の棚卸しも行い、個体識別の管理番号を割り振り、ラベルを貼り、台帳管理できるようになっている。

又、現時点では既存の ActiveDirectory を利用した記録デバイス利用制限になっているが、現在、固体識別管理番号毎の利用制限をするためのソフトウエア導入を進めている。実は、このソフトウエアの追加費用も、USB 利用可能者だけに負担をお願いすると事前に宣言していた事も想定以上に削減が進んだ原因かもしれない。

４．３ その他施策

上記２つの重点施策以外にも、下記のセキュリティ施策も試みている。他社では当然実施済の内容もあるかと思うが、少しでも参考になれば幸いである。

4.3.1）P ドライブ

社内では P ドライブと呼んでいるが、実は個人用のファイルサーバーである。PC 内にはデータは保存させず、この P ドライブに全てのデータを保管してもらっている。結果、PC 紛失時の情報漏洩の心配がほぼ無くなっただけでなく、PC 障害時のデータ消失の心配も無く代替の PC ですぐに業務が継続できるようになった。一人当たりの容量制限も設け、これ以上必要な人からは追加費用を払ってもらっている。　VDI(Virtual Desktop Infrastructure:仮想デスクトップインフラ)システムに比べはるかに安価なこの方式を私は「なんちゃってシンクライアント」と呼んでいる。

4.3.2）メール添付剥ぎ取りツール

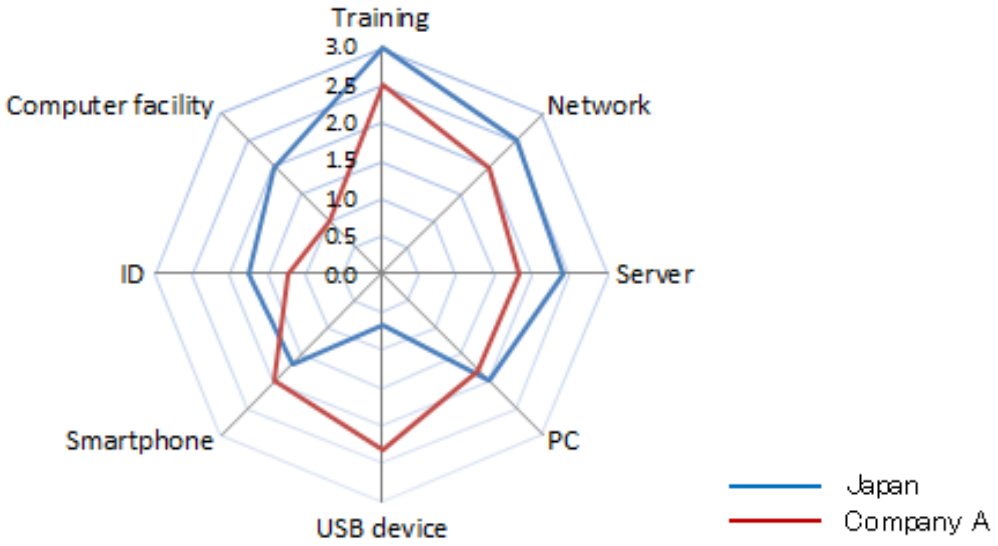
弊社は電子部品の製造販売を行う B to B の企業である。お客様は完成品メーカであり、我々の重要な機密情報の一つにお客様からお預かりする図面などの情報がある。これらはメールでいただく事も多く、このメールの扱いを一つ間違えるとお客様の機密情報が不用意に転送、拡散してしまうリスクがある。機密情報は決められた場所に保管する事になっているが、保管する作業と権限の付与はメールを受け取った人が行う必要があり、運用の徹底に課題があった。そこで、特定のメールドメインから届く添付ファイルをシステムが

自動で引き剥がし、所定のファイルサーバーに保管する仕組みを独自に構築し運用している。権限の付与やアクセスのログもメールの宛先などから自動で設定される仕組みになっている。現在対象のお客様を順次拡大している。

4.3.3)海外拠点のセキュリティレベル調査

これは、数年前に行った施策なのだが、内容を大幅に見直し実施した。３５前後の質問で構成されているが、それらを８つのカテゴリー分類しレーダーチャート（図６参照）で結果を情報セキュリティ管理者間で共有し、自部門のセキュリティ施策計画に反映してもらっている。現場の情報を本社で溜める事なく、広く全社で共有する事で、自部門のセキュリティレベルを認識できるだけでなく、海外現地法人間の施策内容の共有も可能になったと聞いている。

（図６）海外拠点のレーダーチャート例



4.3.4)SaFiT

これは、クラウドを利用したお客様、取引先様との大容量のデータ交換サービスを社内では SaFiT(Safty File Transfer service)と呼んでいる。インターネットメールで送れない大容量のファイルの交換をするためのツールで、USB 記録デバイスの削減にも一役かっている。国内海外を問わず利用が進んでいるが、外部サービスのため費用が高いと現場から改善要望が挙がっている面もある。

4.3.5)サイバー攻撃メール訓練

以前から実施している偽のサイバー攻撃訓練であるが、自社内で独自にメール発信、集計できる仕組みを作成し費用をかけずに行っている。2016 年 3 月までは年１回の実施に留めていたが、4 月以降は 4 半期に一度の頻度にし、メール文面のレベルも直近の実攻撃メールに似せたもので実施してしている。

4.3.6)セキュリティ事故対応訓練

社内の CSIRT 要員向けのウイルス対応訓練を新たに始めている。これは訓練事務局以外には事前に訓練シナリオを知らせずに行う訓練で、CSIRT 要員が正しく連絡や行動ができたかを評価し、改善を促すものである。BCP 対応訓練にヒントを得て、自社内で独自に作成、実施している。
やはりシナリオが事前にわからない事で、対応に苦慮する事が多く見受けられる。但し、これはある意味正しい姿ととらえ、訓練の最後に必ず反省会を行い、失敗を次に活かすようにしている。この訓練は年に２回実施している。

４．４ 事故件数削減結果

これらの施策実行を通じ事故件数は明らかに減少しはじめ、下半期（2015/10-2016/3）の事故件数前年比半減の目標達成に手応えを感じていた。が、2016 年 2 月に実施した USB デバイスの一斉棚卸しで、USB 紛失の事故報告が数件あり、わずかに目標達成には至らなかった。ただ、この一斉棚卸しは昨年度は実施しておらず異常要素と考えれば、目標は達成できた事になる。一方、海外拠点の事故件数は、情報セキュリティ強化の働きかけや月報などにより見える化が進んだ効果？もあり大幅に事故の報告が増えてしまった。ただ海外売上比率が 90%を越える弊社にとっては、ある意味ようやく正しい姿が見えるようになったと考えるべきだと思う。
今期（2016/4～）はこの事件報告やセキュリティレベル調査の結果を受け、海外のセキュリティの弱い地域や子会社への働きかけや支援を増やしている。

５．施策外部評価

上記施策以外に 2016 年 2 月に行った外部企業によるインターネットからの擬似進入テスト（ペネトレーションテスト）も行った。が結果が想定以上に芳しくなく、緊急に各種対応を行った。この経験から、外部評価の重要性を改めて認識し、改めて情報セキュリティの施策内容とレベルを外部企業に評価してもらう事にした。
実は ISO27001 などの公的認証の評価サービスをしていただける企業は多くあるが、情報セキュリティ施策の内容を全般的に評価し、強みや弱みを明示、弱みに対する対策案を複数提示してくれるまでの企業はかなり少なかった。
評価の結果、今後強化すべき点として上げられたのが、情報セキュリティ施策を従来の防御を重点にしたものから、ウイルスの進入を前提にした、検知施策に重点を移していくべきとの指摘であった。現在情報セキュリティ事務局メンバーとこの検討を始めているが、この施策領域はかなりのコスト負担が強いられる事がわかり、施策の優先順位づけが重要と感じている。情報セキュリティ責任者や経営層の理解だけでなく、現在の事務局の体制で運用していけるかも検討課題となっている。

６．日本政府への提言

情報セキュリティに携わり一年半、そして今後も様々な施策に取組む事になるが、我々

一企業にできる対策の限界も感じ始めている。社会に目を向ければ、インターネットに加え、自動運転、ウェアラブルなど IoT なども社会インフラとして浸透しはじめている。今やサイバーセキュリティは各企業の課題のみならず、国家の安全保障問題となっている。一方サイバー攻撃の大部分は海外から届いているとも聞く。

そこで２つの提案をさせていただきたい。

１） ネットワークセキュリティ

海外からの攻撃が増加、高度化している現状を考えると、日本へのネットワークの入り口で政府が一括で不正通信を検知、防御をできないものだろうか？技術的には不可能ではないはずである。勿論各企業でも防御や検知の仕組みは必要だとは思うが、更にネットワーク通信経路の入り口で高度な防御ができれば非常にありがたい。日本には大企業のみならず中小の企業にも機密情報資産が散在している。特に未知のウイルス対策については、コスト面でもハードルが高いと感じる企業も少なくないはずである。

２） 高度情報セキュリティ技術者

現在政府が推奨している、各企業で高度な専門知識を有する技術者の育成と確保にはかなり無理があると感じている。日本にはこの領域の技術者が少ないだけでなく、社内での育成する方法もほとんど無いのが現状である。勿論企業にもある程度の専門家技術者は必要だと思うが、中小企業に至るまでこの人員を採用育成するのにはかなりのハードルであろう。そこで、特に高度な情報セキュリティの専門家は公的機関が一定規模の要員を抱え、社会的にも大きな問題発生時には期間限定で企業の対応を支援していただける体制は作れないものだろうか？

昨今は中国やロシアなどを主とする専門集団が攻撃先や目的を特定しサイバー攻撃を仕掛けてきている。攻撃は益々巧妙になり、未知のウイルスに感染する確率が高まっている。技術的にも体制的にも我々単一企業ができる限界を感じ、この提案をさせていただいた。政府だけでなく産学官共同で総力を挙げてこの問題に取組む価値は十分にあると感じている。

７．終わりに

この論文をまとめる中で様々な取組みをさせていただいた事に改めて気づいた。又、いろいろな施策を通じ結果が残せた事は、様々な助言をいただいた部門セキュリティ管理者担当者の皆様、従業員の皆様、そしてご指導いただいた役員の方々や上司の皆様のおかげであると感謝している。そしてそれ以上に、私という無茶な人間を支えてくれたセキュリティ事務局メンバーの頑張りには特に感謝している。メンバーにはなかなか面と向かって言えないので、この場を借りる。本当にありがとうございました。

実は、当初上司からは 1 年の期限つきと言われていたので今期はお役御免のつもりであったが、もう少しやる事になり、今は事務局メンバーの育成に心を配りながら事にあたっている。情報セキュリティに終わりはない。ただ、立ち止まる事は後退を意味する気の抜けないテーマである。しかし、難しく考えずにシンプルに前向きに明るく取組む姿勢は今後も継続していきたいと思う。

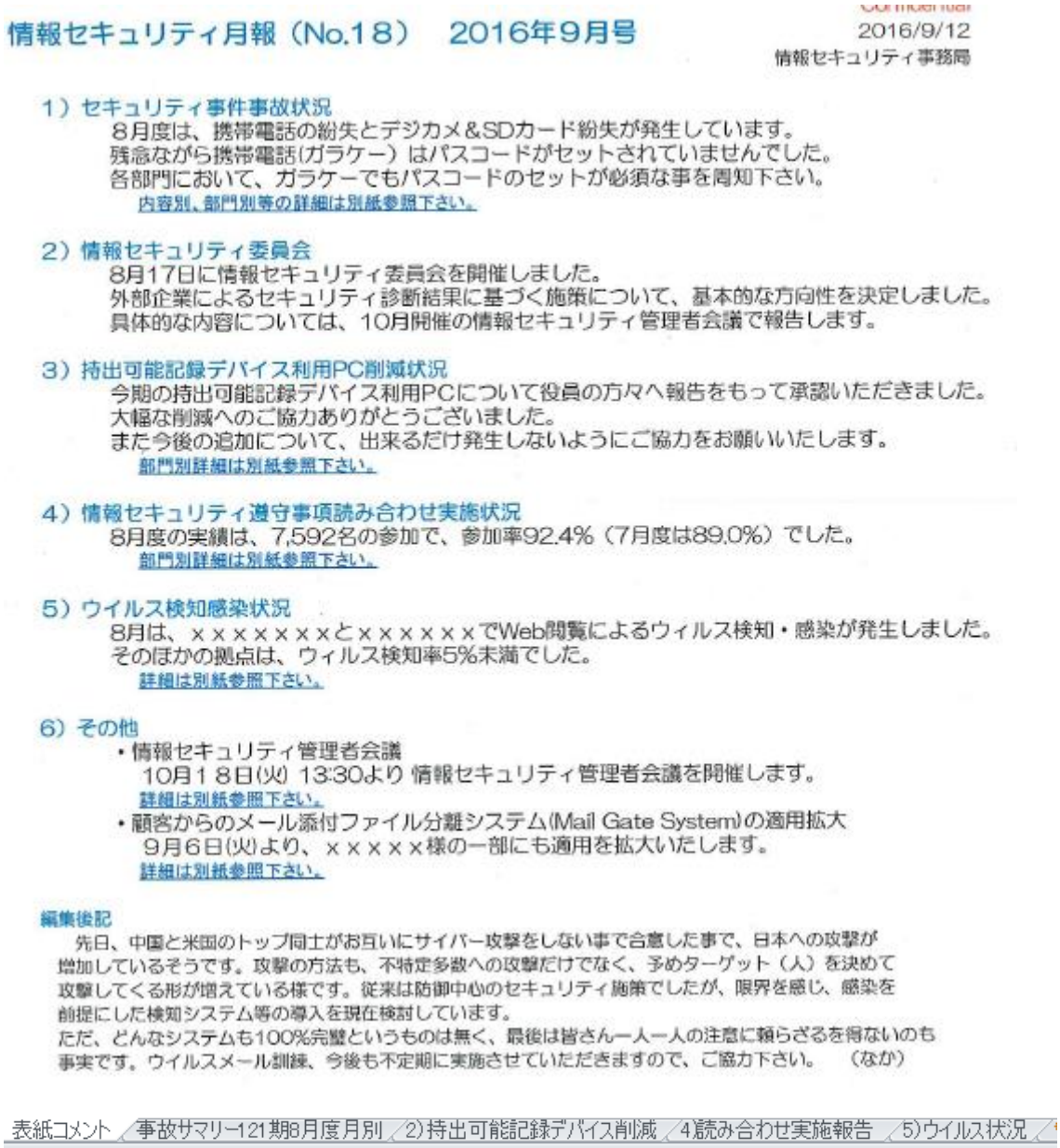
（図７）グローバル主要メンバーと

以上。

以下参考資料

（図８）情報セキュリティ月報例

部門情報セキュリティ組織メンバー及び経営層の皆様にお送りしているもの。



情報セキュリティ月報（No.18）　2016年9月号

Confidential
2016/9/12
情報セキュリティ事務局

1）セキュリティ事件事故状況
8月度は、携帯電話の紛失とデジカメ＆SDカード紛失が発生しています。
残念ながら携帯電話(ガラケー）はパスコードがセットされていませんでした。
各部門において、ガラケーでもパスコードのセットが必須な事を周知下さい。
内容別、部門別等の詳細は別紙参照下さい。

2）情報セキュリティ委員会
8月17日に情報セキュリティ委員会を開催しました。
外部企業によるセキュリティ診断結果に基づく施策について、基本的な方向性を決定しました。
具体的な内容については、10月開催の情報セキュリティ管理者会議で報告します。

3）持出可能記録デバイス利用PC削減状況
今期の持出可能記録デバイス利用PCについて役員の方々へ報告をもって承認いただきました。
大幅な削減へのご協力ありがとうございました。
また今後の追加について、出来るだけ発生しないようにご協力をお願いいたします。
部門別詳細は別紙参照下さい。

4）情報セキュリティ遵守事項読み合わせ実施状況
8月度の実績は、7,592名の参加で、参加率92.4%（7月度は89.0%）でした。
部門別詳細は別紙参照下さい。

5）ウイルス検知感染状況
8月は、ｘｘｘｘｘｘｘとｘｘｘｘｘｘｘでWeb閲覧によるウィルス検知・感染が発生しました。
そのほかの拠点は、ウィルス検知率5%未満でした。
詳細は別紙参照下さい。

6）その他
・情報セキュリティ管理者会議
10月１８日(火) 13:30より 情報セキュリティ管理者会議を開催します。
詳細は別紙参照下さい。
・顧客からのメール添付ファイル分離システム(Mail Gate System)の適用拡大
９月６日(火)より、ｘｘｘｘｘ様の一部にも適用を拡大いたします。
詳細は別紙参照下さい。

編集後記
先日、中国と米国のトップ同士がお互いにサイバー攻撃をしないまで合意した事で、日本への攻撃が増加しているそうです。攻撃の方法も、不特定多数への攻撃だけでなく、予めターゲット（人）を決めて攻撃してくる形が増えている様です。従来は防御中心のセキュリティ施策でしたが、限界を感じ、感染を前提にした検知システム等の導入を現在検討しています。
ただ、どんなシステムも100%完璧というものは無く、最後は皆さん一人一人の注意に頼らざるを得ないのも事実です。ウイルスメール訓練、今後も不定期に実施させていただきますので、ご協力下さい。　（なか）

表紙コメント　事故サマリー121期8月度月別　2)持出可能記録デバイス削減　4)読み合わせ実施報告　5)ウイルス状況

（図９）情報セキュリティ遵守確認シート

読み合せシートの標準版の冒頭部分。他に、標語版、クイズ版、分割版がある。

TDK全社情報セキュリティ遵守確認シート　　2015/10版

TDKにおける情報セキュリティの遵守事項の抜粋版です。
抜粋版ですので、記載されていない事は許可されていると理解しないでください。
疑問質問等は、部門情報セキュリティ管理者、担当者に確認し、指示を受けて下さい

① IT機器、重要書類の紛失には十分気をつけます。
- ・社外持ち出しの際には、体から離しません。電車網棚、車内放置はしません。
- ・スマートフォン、フィーチャーフォンの紛失にも特に気をつけます。
- ・飲酒時には、PC、重要書類は 持ち出しません。
  やむなく持ち出す場合は 上司の了解を得、深酒、二次会参加はしません。
- ・ノートPCは 帰宅時に鍵のかかる場所に保管 又は、盗難対策をします。
- ・万が一紛失してしまったら、24時間以内に 上長 又は 情報セキュリティ管理者、担当者に連絡します。

② 社外に持ち出すIT機器には、決められた設定を行います。